USER OBJECTS FOR AUTHENTICATING THE USE OF ELECTRONIC DATA

[0001] The present application hereby claims priority under 35 U.S.C. §119 on German patent application number DE 103 11 327.4 filed March 14, 2003, the entire contents of which are hereby incorporated herein by reference.

Field of the Invention

[0002] The invention generally relates to an electronic data processing facility for the editing, storage and reading of electronic data by different users who are granted different data access rights and whose data access operations are documented. The invention also generally relates to a method for operating a data processing facility and to a storage medium with information for carrying out such a method on a data processing facility.

Background of the Invention

[0003] Text data and image data, particularly data having a medical relevance, such as findings, diagnostic images or patient data, are increasingly being stored and handled electronically. Electronic handling requires particular measures for making data access operations and data alterations reconstructable. Particularly in the health sector, a large amount of electronic data can be classified as confidential and requires data protection provisions to the effect that any user of electronic data is clearly identified and authenticated. Any data access or any use of the data needs to be clearly documented with an indication of the user ("auditing"), and access to data connected

with patients must be granted only to authenticated users ("access control").

[0004] Thus, identification represents explicit, individual identification of the user, while authentication refers to the approval of particular data access rights for the user. Authentication thus means authorization of the user for particular data access rights. Authentication fundamentally presupposes identification.

[0005] This gives rise to the following demands: for clear documentation, it is necessary for every user to be individually identifiable. To protect the data against unauthorized access, mechanisms on different software levels are conceivable, with the ability to bypass these mechanisms being dependent on the respective depth of the software level. Mechanisms executed on lower software levels, that is to say at operating system level in the extreme case, permit few opportunities for bypass and therefore ensure more secure access protection.

[0006] Therefore, access rights when handling security-critical or medically relevant data, particularly personal data and patient data, are implemented at operating system level as far as possible. This requires that a user who is intended to enjoy comprehensive access rights be logged onto a system which is able to grant access to the data as an operating system user. By contrast, a user who is intended to enjoy less comprehensive access rights needs to be logged on merely as an application user in the application software.

[0007] One possible system for handling electronic data might be a medical workstation, for example a

"modality" which is able to record and edit findings data and image data. Typically, such a workstation is used by a plurality of people at short intervals of time, and these people respectively alternate quickly between looking after the patient and using the appliance. Hence, one and the same workstation is used by a plurality of users in quick succession who look after a plurality of patients. It is obvious that, from the point of view of rationalization and economy of work operations, changing between various users and various patients should take place as quickly as possible.

[0008] Other systems for handling confidential electronic data are used, by way of example, in research, in the financial sector, in law or in demographic matters. In principle, personal data and data requiring secrecy need to be regarded as confidential to the same degree.

[0009] Since the data in question are generally regarded as being needy of protection to a particular degree, it is demanded that the users be authenticated as securely as possible. On the basis of what has been said above, authentication should thus be implemented at operating system level. The result of this is that it is possible to change between different users only by logging on to the operating system again.

[0010] In the systems used today, however, logging onto the operating system again is very time-consuming, since it requires that the operating system be restarted every time and, in addition, that the application program used to edit the data be terminated and restarted every time as well. The time-consuming restart makes implementing the greatest possible access security on workstations which are to be used on a frequently and rapidly changing basis too time-

consuming and therefore unacceptable in practical applications which are frequently confronted by time pressure.

[0011] Conventional medical workstations and other workstations operating with confidential data therefore have data protection systems which usually either prevent multiple use of the workstation from the outset or provoke deliberate bypassing of the security system in daily use under time pressure by inducing various users to dispense with respectively logging onto the system again by using one and the same common system logon. The use of a common system logon also has the effect that it becomes more difficult to document user data in connection with access operations to the security-critical data, since the system cannot individually identify different users using the same system logon.

SUMMARY OF THE INVENTION

[0012] An object of an embodiment of the invention is to specify a system for editing, storing and reading electronic data which allows faster change of users, with no less data protection, and in which full identification for documentation purposes and for correctly authenticating individual users is made possible.

[0013] An embodiment of the invention achieves this aim by way of a data processing facility, by way of a method for operating such a facility and by way of a storage medium with information for carrying out such a method on a data processing facility.

[0014] An embodiment of the invention is based on the insight that different users of a workstation operating with confidential electronic data frequently belong to

the same authentication level, i.e. have the same access rights to the data in question. In the context of data protection in the health sector, the users in a common authentication level can be regarded as one administrative team, for example, whose access rights are defined as team or group access rights.

[0015] To date, a user has needed to be logged onto the system as a standard, individual user object which is used for documentation and authentication purposes. An embodiment of the invention decouples the conventional connection between identification object and authentication object. Instead, it uses an individual documentation user object, which contains information for identifying a user, and a separate authentication user object, which defines a particular authentication level. The authentication user object can be allocated on a non-individual basis to all users of an identical authentication level and in this regard can be considered to be a group user object for user groups.

[0016] The use of the separate user objects makes it possible to change between users on a common authentication level, e.g. in an administrative team, by changing the individual documentation user object, without inevitably also needing to restart the operating system on account of a related change of authentication user object. By way of example, the change between user objects belonging to a common user group can be made at the level of a piece of medical or personal application software for data editing. Only when changing between users in different user groups is it also necessary to change the authentication level, that is to say to log off and log on again at operating system level.

BRIEF DESCRIPTION OF THE DRAWINGS

[0017] The present invention will become more fully understood from the detailed description of preferred embodiments given hereinbelow and the accompanying drawing, which is given by way of illustration only and thus are not limitative of the present invention, and wherein:

FIGURE 1 shows a schematically illustrated data processing facility,

FIGURE 2 shows a flowchart,

FIGURE 3 shows user levels.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0018] Figure 1 shows the architecture of a preferred embodiment of the electronic data processing facility. The central element in this data processing facility, which may be a medical workstation, a research workstation or a financial terminal, for example, is a computer 1 which has an input unit 9, e.g. a keyboard, and an output unit 11, e.g. a screen.

[0019] The computer 1 has access to a data store 3 for storing personal or medically relevant (that is to say that they need to be classified as confidential) electronic data. The computer 1 runs an operating system (in the normal way) which is required for configuring the hardware and for operating the computer 1. In addition, the computer 1 runs an application program which is suitable for handling the confidential image data, text data, or metadata. The application program can be used, by way of example, for inputting

patient data, for inputting medical findings or written reports, for editing diagnostic image data or for recording personal information. Users of the program may be medical specialist personnel or patients, or else administrative personnel, technicians, purchasers, researchers or financial specialists. The computer 1 allows the electronic data to be processed, where processing is intended to mean generation, storage, alteration, deletion or reading and any other data access.

[0020] The computer 1 also has access to a documentation memory 5 which documents all access operations to the data in the data store 3. For this purpose, information about the type of access, the accessed data and the accessing user is stored, where access to the data should be regarded not just as alteration but also as simple viewing thereof.

[0021] The computer 1 is also connected to an authentication memory 7 which may be arranged at a central location either with a direct connection or remotely from the computer 1 and can be accessed using a data communication link 8. The authentication memory 7 contains information which allows a user of the computer 1 or of the entire data processing system to be identified as a user, to be assigned a user object which he can use to log onto the system, and which makes it possible to establish to which user group the user object belongs. In this case, the user group contains information which defines the authentication level applicable to the user object. In other words, the user object can be assigned and granted access rights using the association with a user group, and hence can be authenticated.

[0022] To be able to identify a user of the system and assign him a user object, the computer 1 needs to check information about the user which it can compare with the information in the authentication memory 7. Since the result of this identification is that documentation data are generated and the user's authentication level is stipulated, the actual information to be checked needs to be handled particularly confidentially and protected. The check can therefore be made in the form of a password check.

[0023] The use of passwords is known to have the drawback that sufficiently secure passwords are generally long, difficult to remember and complex to input. This complicates use and particularly the rapid changing of users on the system. More practical alternatives to a password check involve using a camera 13 to record biometric data for the user, e.g. the form of his iris, using a key reader 15 to scan a user-specific electronic or mechanical key, or using a chip card reader 17 to check a user-specific chip card. The proposed security systems allow secure identification without any complexity for the user, with, in particular, the check on biometric data being particularly user-friendly and deception proof.

[0024] The authentication memory 7 can advantageously be positioned centrally at a remote location from the workstation. This allows it to be used as a data server for an entire building, e.g. a hospital or an office building, or across buildings. When positioned centrally as an authentication server, it can operate in the manner of a trust center using asymmetrical key systems. When using an asymmetrical key system with a public and a private key, there is also no need to operate the data communication link 8 in encrypted form. It goes without saying that adequate protective

measures, such as firewalls, need to be provided in order to protect the data in the data store 3 or in the entire system.

[0025] The use of a central authentication server increases the portability of the data and also allows the use of expert systems with access to the data by experts working at separate locations, since the documentation and authentication would not be locally restricted. In addition, it would be possible to define and prescribe standards for the various authentication levels centrally in order to be able to use them on a standard basis in the entire data system, for example for the entire health sector.

[0026] The operating system running on the computer 1 is used, in a known manner, for configuring the hardware of the computer. It decides what hardware components are available and which users are able to access these components. This allows it to enable, disable or authorize the use of the hardware and hence also of the data stored in the hardware on a user-dependent basis. In addition, the operating system is used as a platform on which application programs can run, in which case it inevitably also authorizes the access rights for the application programs themselves. Since the application programs work on the basis of the operating system, it is possible to terminate and start them while the operating system is running. By contrast, altering the valid authentication level with maximum data protection is possible only by terminating and restarting the operating system.

[0027] Figure 2 shows the method steps according to which an embodiment of the invention operates in the form of a flowchart. The flowchart shows the workflows executed by the operating system and the application programs.

In step 31, a user first of all logs on for the purpose of using the system, e.g. the medical workstation. In this case, logon is performed in a known manner by inputting a user identifier using a keyboard or another suitable input unit. The user identifier is the same as a login or a logon name and provides no kind of data protection.

[0028] On the basis of a user's logon, a security check is performed in step 33. The security check is used to identify a user in a deception proof manner and is therefore the same as inputting a user password. It can be in the form of password input using a keyboard, or instead biometric data for the user can also be ascertained using a camera, or a mechanical or electronic key or a chip card can be scanned using a checking unit connected to the system.

[0029] Depending on the type of security check in step 33, it may be possible to dispense with the input of a user identifier in the preceding step 31. By way of example, an automatically performed biometric test allows full and secure identification to be performed without any action by the user in step 31. The use of a sufficient secure key may be sufficient for recognizing the user and for verification at the same time, that is to say as an actual security check. This simplifies frequent user changes on the system, in particular, because complex keyboard inputs can be dispensed with.

[0030] In step 35, the previously recognized user is identified as a user object by a program working at the level of the operating system. The system accesses a data stock which allows users to be recognized on the basis of the data ascertained in the security check. This data stock may either be stored within the system or may be accessible using remotely accessible data,

e.g. using the Internet. It is also possible to use local and nonlocal data in parallel.

[0031] In the next step 37, it is established to which user group the previously identified user object belongs. To this end, data which may likewise be stored locally or nonlocally are accessed. The data stocks for identifying user objects and for assigning them to user groups may be stored either in the same data store or in separate data stores.

[0032] In step 39, a check is carried out to determine whether the user group connected with the user object which currently needs to be logged onto the system corresponds to the one connected with the user object logged on beforehand, or whether the user object belongs to a different user group. If there is a match between the user group which is currently to be logged on and the user group logged on beforehand, the system starts the application program desired by the user in step 49. Otherwise, it is necessary to restart the system, since the change of user group is associated with a change of authentication level, which can be implemented only by changes at operating system level.

[0033] To this end, the current configuration of running application programs is buffer-stored in step 41, and the application programs are terminated in step 43. In step 45, the current status of the operating system is buffer-stored, and the operating system is terminated and restarted in step 47.

[0034] The buffer-stored data relating to the status of the operating system and the configuration of the applications allow the previous workstation configuration to be restored after the operating system is restarted. In this case, the user identified

beforehand at logon can automatically be logged onto the operating system, and the associated authentication level can be set. Alternatively, the user can be asked to log on again in step 31. This requires repetition of the security check in step 33, the identification as a user object in step 35 and the assignment to a user group in step 37. Following successful authentication, the previous configuration of the application programs or a desired application is started in step 49.

[0035] In step 51, the application program establishes whether the user object currently logged on matches the one which is to be logged on anew, or whether a change has taken place. If a change has taken place, the now valid user object is entered again in step 53 at the level of the application program and can now be retrieved for documentation purposes at any time, otherwise the previous user object remains active.

[0036] In step 55, the user's data access operations to the confidential data are documented. This involves documenting which user uses which application program to access which data at what time. In addition, the type of data access is documented, i.e. a record is made of whether the data have been edited or merely viewed.

[0037] The flowchart in Figure 2 makes it clear that the invention simplifies the changing of users on the system. In conventional systems, steps 41 to 49 for restarting operating systems and application programs need to be executed for every change of user, in which case particularly step 47, in which the operating system is restarted, is particularly time-consuming. By contrast, an embodiment of the invention makes it possible to dispense with these steps whenever it is established that the authentication level or the

authentication user object connected with the user who is to be logged on anew matches that of the user who is currently logged on. This always involves dispensing with restarting the operating system and, at most, restarting the application program in order to change the documentation user object.

[0038] Generally, however, it will be possible to dispense with restarting the application program in order to change the documentation user object. Instead, the new user object is recorded only within the application.

[0039] Figure 3 illustrates the isolation between operating system and application level, which an embodiment of the invention uses to advantage. In Figure 3, the operating system 71 is on the level above the dashed line, which is isolated from the level of the application programs 73 below the dashed line.

[0040] The operating system 71 is responsible for configuring the hardware of the data processing facility and for identifying and authenticating a system user. To this end, the operating system has an authentication entity 75 which is either part of the operating system or operates at the level of the operating system in order to be able to prescribe a different authentication level according to the user object. The hardware configuration associated with an authentication level and the respective scope of access rights are defined in user groups 77 in this case. Each user group 77 defines a dedicated authorization level and a dedicated hardware configuration. The authentication user object and hence the user group 77 are changed at the level of the operating system 71.

[0041] At the level of the application programs 73, the data access operations permitted in line with the allocated authentication level take place and are documented by the documentation entity 79. The documentation entity 79 records which user has accessed which data in what manner at what time. Both data access operations for altering the data and those for merely viewing the data are documented. The scope of documentation corresponds at least to the legal stipulations in force which have been prescribed to the data. To record the user who is accessing data, the documentation entity 79 requires information in order to identify him. This information is provided by the respective documentation user object 81 logged on, whose identifier is stored as the originator of any data access.

[0042] The user objects 81 are each part of a user group 77. A change of user object 81 does not have to entail a change of authentication level, i.e. it may be made without changing the user group 77 and merely at the level of the application program 73. To clarify this, Figure 3 respectively shows a plurality of user objects 81 within a user group 77 at the level of the application program. From the illustration, it can be seen that just changing to a user object 81 in a different user group 77 also necessitates changing the user group and hence a change at the level of the operating system. Only in such cases does it become necessary to restart the operating system 71, and this may entail changing the authentication level, which results in the authentication entity 75 granting the application program 73 a different scope of access rights.

[0043] The scope of data access rights is thus prescribed by the operating system level, while data access

operations are documented exclusively at application program level.

[0044] A program may further be adapted to interact with an electronic data processing facility in order to carry out the method of an embodiment of the present application. The program may be stored on a storage medium on which the program information is stored.

[0045] The program can be offered in the form of a computer-readable storage medium. The storage medium may be a built-in medium installed inside a computer main body or removable medium arranged so that it can be separated from the computer main body. Examples of the built-in medium include, but are not limited to, rewriteable involatile memories, such as ROMs and flash memories, and hard disks. Examples of the removable medium include, but are not limited to, optical storage media such as CD-ROMs and DVDs; magneto-optical storage media, such as MOs; magnetism storage media, such as floppy disks (trademark), cassette tapes, and removable hard disks; media with a built-in rewriteable involatile memory, such as memory cards; and media with a built-in ROM, such as ROM cassettes.

[0046] Exemplary embodiments being thus described, it will be obvious that the same may be varied in many ways. Such variations are not to be regarded as a departure from the spirit and scope of the present invention, and all such modifications as would be obvious to one skilled in the art are intended to be included within the scope of the following claims.